

Über die endliche Erzeugbarkeit verallgemeinerter Einheitengruppen

von

HELMUT BEHR

1961

Über die endliche Erzeugbarkeit
verallgemeinerter Einheitengruppen

Inauguraldissertation

zur

Erlangung der Doktorwürde

der

Hohen Naturwissenschaftlichen Fakultät

der

Ludwig-Maximilians-Universität

zu München

Vorgelegt

von

Helmut Behr

aus

München

Januar 1961



Berichterstatter: Prof. Dr. M. Kneser

Tag der mündlichen Prüfung: 22.2.1961

Fotodruck: Mikrokopie G.m.b.H. München 2, Weinstr. 4

INHALTSVERZEICHNIS.

Einleitung	1
Abschnitt I: Beweis der allgemeinen Sätze (über Definierbarkeit von Gruppen durch endlich viele Elemente)	6
1. Beweis von Satz 2	6
2. Beweis von Satz 3	12
3. Beweis von Satz 4	13
Abschnitt II: Lineare und orthogonale Einheitsgruppen	21
1. Allgemeine lineare Gruppe	21
2. Spezielle lineare Gruppe	25
3. Orthogonale Gruppe	27
Abschnitt III: Ausdehnung der Resultate auf einige weitere Gruppen	36
1. Lineare und orthogonale Einheitengruppen über einem algebraischen Zahlkörper	36
2. Unitäre und symplektische Einheitengruppen	39
Literaturverzeichnis	46

Einleitung.

Der Dirichletsche Einheitensatz besagt im wesentlichen, daß die Gruppe der Einheiten eines algebraischen Zahlkörpers K direktes Produkt von einer endlichen Gruppe von Einheitswurzeln und endlich vielen freien zyklischen Gruppen ist. Er gibt darüber hinaus ihre Anzahl an. Dieser Satz wurde von Hasse und Chevalley in folgender Weise verallgemeinert: Sei S eine endliche Menge von Primdivisoren von K . Dann bildet die Menge aller Elemente aus K , in deren Primdivisorzerlegung nur die Primdivisoren aus S mit von Null verschiedenem Exponenten auftreten, eine Gruppe U_S , die Gruppe der relativen Einheiten bezüglich S . (Im Fall des rationalen Zahlkörpers Q kann man U_S einfach beschreiben als die Menge aller Zahlen aus Q , deren Zähler und Nenner prim sind zu allen nicht in S gelegenen Primzahlen). Die Gruppe U_S ist direktes Produkt von einer endlichen Gruppe von Einheitswurzeln und endlich vielen freien zyklischen Gruppen.¹⁾

Einheiten lassen sich bekanntlich auch in einer multiplikativen Gruppe von Matrizen erklären, deren Matrixelemente einem Körper entnommen sind, in dem ein Ring ganzer Elemente ausgezeichnet ist. So kann man z.B. die Elemente der unimodularen Gruppe (das sind die ganzzahligen Matrizen mit Determinante $+1$ oder -1) als Einheiten der allgemeinen linearen Gruppe über dem Körper Q der rationalen Zahlen auffassen; ist s die Matrix einer quadratischen Form mit Koeffizienten aus Q , so nennt man die Gesamtheit der Lösungen x der Matrixengleichung $x^T s x = s$ die orthogonale Gruppe bezüglich s und die Untergruppe mit

¹⁾ Einen Beweis findet man in (14), p.168.

ganzrationalen Matrixelementen die Einheitengruppe von s . Da es sich hier um nichtabelsche Gruppen handelt, kann man eine ähnlich genaue Strukturbeschreibung wie oben nicht erwarten. Von den beiden genannten Einheitengruppen konnten Minkowski (in (6) bzw. in (7), Band 2, S.53) bzw. Siegel (in (11)) immerhin zeigen, daß sie endlich erzeugbar sind. Man kann ihre Beweise als Anwendungen eines allgemeinen Prinzips ansehen, das erst später von Siegel explizit formuliert wurde und das man so aussprechen kann:

Satz 1. Ist T ein zusammenhängender Hausdorffscher Raum, G eine Gruppe von Homöomorphismen von T , D eine offene Teilmenge von T mit der Eigenschaft $GD = T$ und bezeichnet E die Menge aller Elemente aus G , für die D und gD einen nichtleeren Durchschnitt haben, so wird G von den Elementen aus E erzeugt.
Insbesondere ist G endlich erzeugbar, wenn E endlich ist. ²⁾

Man wird sich fragen, ob man die genannten Gruppen durch endlich viele Relationen zwischen ihren Erzeugenden definieren kann. Diese Frage wird in einer Arbeit von Gerstenhaber (in (2)) unter ähnlich allgemeinen Voraussetzungen wie in Satz 1 untersucht, der dort bewiesene Satz ist aber hier nicht anwendbar. Man kann jedoch mit derselben Beweisidee auch den folgenden Satz gewinnen, der dann für die linearen und orthogonalen Einheitengruppen das gewünschte Resultat liefert.

²⁾ Einen Beweis findet man in (12), vgl. Lemma 8 und Abschnitt 9

Satz 2. Es seien die gleichen Voraussetzungen wie in Satz 1 erfüllt, die Menge E sei endlich; darüber hinaus sei T lokal zusammenhängend und einfach zusammenhängend. Dann kann die Gruppe G durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden.

Die eingangs erwähnte Verallgemeinerung des Dirichletschen Einheitensatzes legt außerdem die Frage nahe, ob die Sätze von Minkowski und Siegel einschließlich der Aussage über die Relationen auch dann gültig bleiben, wenn man als Matrixelemente statt ganzer Zahlen auch solche rationalen Zahlen zuläßt, bei denen in der Primfaktorzerlegung des Nenners nur Potenzen von Primzahlen aus S auftreten; dabei bezeichne S wieder eine beliebig vorgegebene endliche Menge von Primzahlen. Diese Frage wird in der vorliegenden Arbeit bejaht. Der Beweis wird durch Induktion nach der Anzahl der Elemente von S geführt. Die Sätze von Minkowski und Siegel dienen dabei als Induktionsanfang, während beim Induktionsschritt die folgenden Sätze 3 und 4 angewandt werden. Sie übertragen die durch die Sätze 1 und 2 beschriebene Beweismethode auf diskrete metrische Räume.

Satz 3. Gegeben sei eine Menge $M = \{A, B, \dots\}$, in der ein ganzzahliger Abstand $d(A, B)$ erklärt ist³⁾, und eine auf M transitiv operierende Gruppe $G = \{a, b, \dots\}$, die den Abstand invariant läßt. Ferner seien die folgenden Bedingungen erfüllt:

³⁾ Die Annahme „ganzzahlig“ ist wegen Voraussetzung b) keine Einschränkung gegenüber einem beliebigen diskreten metrischen Raum.

- a) Es gibt eine Konstante K , so daß man zu zwei beliebigen Punkten A, B aus M mit $d(A, B) > K$ einen Punkt C aus M finden kann mit $d(A, C) \leq K$ und $d(C, B) < d(A, B)$.
- b) Für festes A aus M und eine beliebige Konstante L ist die Anzahl der Punkte B aus M mit $d(A, B) \leq L$ endlich.
- c) Die Fixgruppe U eines Elements aus M ist endlich erzeugbar.

Dann ist G endlich erzeugbar.

Satz 4. Die Bedingungen von Satz 3 seien zu den folgenden verschärft:

- a) Es gibt eine Konstante K , so daß Bedingung 3a) erfüllt ist und man außerdem zu drei beliebigen Punkten A, B, C aus M mit $\min \{d(A, B), d(B, C), d(C, A)\} > K$ einen Punkt D aus M finden kann mit $d(A, D) \leq K$ und $d(D, B) < d(A, B)$ sowie $d(D, C) \leq \max \{d(A, C), d(B, C)\}$.
- b) Bedingung 3b) ist erfüllt.
- c) Die Fixgruppe U eines Elements aus M kann durch endlich viele Relationen zwischen ihren (endlich vielen) Erzeugenden definiert werden.

Dann kann auch G durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden.

Die Beweise für die allgemeinen Sätze 2 - 4 werden wir in einem ersten Abschnitt angeben. Im zweiten Abschnitt wollen wir

diese Sätze dann auf die linearen und orthogonalen Einheitsgruppen über dem Körper Q der rationalen Zahlen anwenden. Im dritten und letzten Abschnitt soll schließlich kurz skizziert werden, wie sich die Ergebnisse auf andere Gruppen ausdehnen lassen. Dabei werden wir zunächst zeigen, daß wir bei den linearen und orthogonalen Gruppen anstelle von Q einen beliebigen algebraischen Zahlkörper zugrunde legen können. Den Beweis der endlichen Erzeugbarkeit der gewöhnlichen Einheitengruppen verdankt man für diesen allgemeinen Fall P.Humbert (3) bzw. Ramanathan (8) , (9) .

Dagegen scheint für unitäre und symplektische Gruppen in der Literatur kein vollständiger Beweis für dieses Resultat vorzuliegen, wenn man einen beliebigen algebraischen Zahlkörper zugrundelegt. Man vergleiche jedoch die Arbeiten von Ramanathan (8) , (10) und Siegel (13). Man kann aber in all den Fällen, in denen man dieses Ergebnis besitzt, auch die Aussagen über die Relationen und die verallgemeinerten Einheitengruppen beweisen.

Herrn Professor Dr.M.Kneser danke ich herzlich für die Anregung zu dieser Arbeit und eine Reihe wertvoller Ratschläge bei ihrer Durchführung.

Abschnitt I :

BEWEIS DER ALLGEMEINEN SÄTZE.

1. Beweis von Satz 2. Wir wollen zunächst erläutern, weshalb es nötig ist, den Satz von Gerstenhaber (in(2)) abzuändern. Er unterscheidet sich von Satz 2 einerseits durch zwei zusätzliche Voraussetzungen, gibt dafür aber andererseits die definierenden Relationen explizit an. Gerstenhaber nimmt nämlich an, daß es im Raum T einen zusammenhängenden Unterraum D gibt, so daß T disjunkte Vereinigung von allen Mengen gD ist, wenn g die Gruppe G durchläuft. Die Voraussetzung „disjunkt“ ist aber in den wichtigsten Anwendungsfällen nicht erfüllt, sie ist jedoch auch für den Beweis des Satzes von Gerstenhaber nicht nötig. Läßt man sie weg, so kann man D als offen voraussetzen und den Beweis dadurch vereinfachen. Es erscheint zweckmäßig auch die Voraussetzung des Zusammenhangs von D zu streichen, weil es manchmal recht mühsam ist, die Existenz eines solchen D nachzuweisen. Man muß dann in Kauf nehmen, daß bei den definierenden Relationen außer den (unten definierten) lokalen noch endlich viele weitere auftreten, die man nicht so einfach beschreiben kann. Betont man nur die Endlichkeit, so kommt man zur Formulierung von Satz 2. Infolge dieser Abänderungen weicht auch die Ausführung des Beweises stark ab; wir wollen deshalb einen vollständigen Beweis von Satz 2 angeben.

Nach Satz 1 ist die Gruppe G endlich erzeugbar und die dort definierte Menge E der Elemente e_i aus G mit der Eigenschaft $e_i D \cap D \neq \emptyset$ ist ein endliches Erzeugendensystem. Durch die Zu-

Ordnung $e_i \rightarrow \bar{e}_i$ bilden wir E umkehrbar eindeutig auf eine Menge $\bar{E}$ ab und nennen die von $\bar{E}$ erzeugte freie Gruppe F . Dann ist G isomorph einer Faktorgruppe von F nach einem Normalteiler R , dessen Elemente wir als Relationen bezeichnen. Liegt das Produkt $e_k = e_i e_j$ zweier Elemente aus E wieder in E , dann nennt man das Produkt $\bar{e}_i \bar{e}_j \bar{e}_k^{-1}$ in F eine lokale Relation. Die lokalen Relationen und eine endliche Menge weiterer Relationen, die wir erst im Lauf des Beweises festlegen werden, erzeugen einen in R enthaltenen Normalteiler N . Die Faktorgruppe von F nach N heie H ; dann gibt es zwei Homomorphismen s von F auf H bzw. t von H auf G . Unser Ziel ist es zu zeigen, da eine geeignet bestimmte Gruppe H isomorph zu G ist. Zu diesem Zweck konstruieren wir nun zu H einen Überlagerungsraum S von T .

Wir definieren zunächst $\bar{S}$ als die Menge aller Paare (x, h) mit x aus D und h aus H . In $\bar{S}$ führen wir eine Äquivalenzrelation $\sim$ wie folgt ein: $(x, h) \sim (x', h')$ dann und nur dann, wenn es ein Element e aus E gibt mit $h' = h s(\bar{e})$ und $x = e x'$. Da in H die Beziehung $s(\bar{e}_i) s(\bar{e}_j) = s(\bar{e}_k)$ gilt, wenn in G die Beziehung $e_i e_j = e_k$ besteht, folgt, da die Relation $\sim$ transitiv ist. Wir definieren nun S als die Menge $\bar{S}$ mit $\sim$ als Gleichheitsdefinition.

Mit Hilfe des Homomorphismus t von H auf G , kann man eine Abbildung $\bar{p}$ von $\bar{S}$ auf T definieren durch die Festsetzung: $\bar{p}(x, h) = t(h)x$; ferner liefert jedes Element h_0 aus H eine Abbildung von $\bar{S}$ auf sich durch $h_0(x, h) = (x, h_0 h)$. Man rechnet sofort nach, da damit auch eine Abbildung p von S auf T bzw.

für jedes Element der Gruppe H eine Abbildung von S auf sich gegeben ist. Die Menge aller Paare $(x, 1)$ in $\bar{S}$ bzw. in S bezeichnen wir mit $\bar{B}$ bzw. B ; $\bar{B}$ und B werden durch die Abbildungen $\bar{p}$ bzw. p umkehrbar eindeutig auf D abgebildet. Außerdem lassen sich $\bar{S}$ bzw. S als Vereinigung aller Mengen $h\bar{B}$ bzw. hB schreiben, wenn h die Gruppe H durchläuft. Sowohl in $\bar{S}$ wie in S läßt sich in naheliegender Weise eine Topologie einführen: in $\bar{S}$ durch die Forderung, daß jede Menge $h\bar{B}$ homöomorphes Bild von D sein soll (wodurch eine Basis der offenen Mengen gegeben wird), in S durch die Quotiententopologie bezüglich der natürlichen Abbildung von $\bar{S}$ auf S . Aus der Definition der Quotiententopologie folgt nun unmittelbar, daß p eine stetige und offene Abbildung ist und daß H eine Gruppe von Homöomorphismen von S ist.

Wir wollen nun zu jedem Punkt x aus T eine Umgebung U bestimmen, die schlicht überlagert wird, d.h. daß jede Zusammenhangskomponente des Urbilds von U durch p homöomorph auf U abgebildet wird. Wir zeigen, daß wir hierfür eine offene Menge der Form gD' wählen können, wo g so bestimmt ist, daß x in gD liegt und D' die Zusammenhangskomponente von $g^{-1}x$ in D ist. Um dies zu beweisen, genügt es offenbar das Urbild von D zu untersuchen. Wir behaupten: Das Urbild $\bar{p}^{-1}(D)$ ist die disjunkte Vereinigung aller Mengen kB , wenn k den Kern des Homomorphismus t von H auf G durchläuft und daher $\bar{p}^{-1}(D')$ die disjunkte Vereinigung der Mengen $k(B \cap \bar{p}^{-1}(D'))$).

Liegt $p(x, h) = t(h)x$ in D , ist aber $t(h) \neq 1$, so ist wenigstens $t(h)D \cap D \neq \emptyset$; somit gibt es ein Element e aus E , so daß

$t(h) = e$ ist. Dann ist das Element (x', h') mit $x' = e x$ und $h' = h s(\bar{e})^{-1}$ gleich dem Element (x, h) und h' liegt im Kern von t , denn es gilt: $t(h') = t(h) t(s(\bar{e})^{-1}) = e e^{-1} = 1$.

Gilt für zwei Elemente k und k' aus dem Kern von t die Gleichheit $(x, k) = (x', k')$, dann gibt es nach Definition ein Element e aus E , so daß die Beziehung $k' = k s(\bar{e})$ besteht. Wendet man t auf diese Gleichung an, so folgt $e = 1$ und damit $k = k'$ und $x = x'$.

Ist D zusammenhängend, so folgt leicht, daß auch S zusammenhängend ist. Da auch der lokale Zusammenhang von T vorausgesetzt war, ist dann S ein Überlagerungsraum von T . Man hat in diesem Fall zur Definition von H nur die lokalen Relationen nötig: dies ist das Resultat von Gerstenhaber. Wegen des einfachen Zusammenhangs von T sind nämlich S und T homöomorph; daraus folgt, daß G isomorph zu H und $N = R$ ist. Nimmt man an, daß D endlich viele Zusammenhangskomponenten besitzt, dann kann man auch eine zusammenhängende Menge D' finden, die dieselben Eigenschaften wie D hat.

Macht man diese Annahme nicht, so wird der Beweis etwas komplizierter. Wir bezeichnen die Menge aller Zusammenhangskomponenten von Bildern von D (unter der Gruppe G) mit M . Nun wählen wir eine Zusammenhangskomponente D_0 von D aus und setzen $\{D_0\} = M_0$. Mit M_1 bezeichnen wir die Menge derjenigen Elemente von M , die mit D_0 Punkte gemeinsam haben. Die Menge aller Elemente von M , die mit wenigstens einem Element von M_1 Punkte gemeinsam haben, aber nicht zu M_0 gehören, nennen wir M_2 ; entsprechend werden

$M_3, M_4, \dots$ definiert. Ferner sei $M' = \bigcup_{i=0}^{\infty} M_i$ und $M'' = M - M'$. Als Teilmengen von T betrachtet sind M' und M'' offen, ihr Durchschnitt ist leer und ihre Vereinigung ganz T . Da aber T zusammenhängend ist, muß schon $M' = T$ sein. Man kann daraus schließen, daß man ein beliebiges Element aus M „durch eine Kette aus endlich vielen Elementen aus M mit D_0 verbinden kann“; d.h. zu Z aus M gibt es Elemente $Z_0, \dots, Z_m$ aus M mit $Z_0 = D_0, Z_m = Z$ und $Z_k \cap Z_{k+1} \neq \emptyset$ für $k = 0, 1, \dots, m-1$.

Durch Induktion nach m zeigt man nun, daß man zu jedem Element Z_m aus M eine Zusammenhangskomponente D_m von D und Elemente $f_1, \dots, f_m$ aus E finden kann, so daß die Beziehung $f_1 \dots f_m D_m = Z_m$ gilt. Sei nämlich $Z_{m-1} = f_1 \dots f_{m-1} D_{m-1}$, dann ist $[D_{m-1} = f_{m-1}^{-1} \dots f_1^{-1} Z_{m-1}] \cap f_{m-1}^{-1} \dots f_1^{-1} Z_m \neq \emptyset$. Also folgt nach Definition von E , daß es ein Element f_m aus E und hierzu eine Zusammenhangskomponente D_m von D gibt, so daß die Gleichung $f_m D_m = f_{m-1}^{-1} \dots f_1^{-1} Z_m$ besteht.

Diese Aussagen wenden wir nun auf die endlich vielen Bilder $e_i D_0$ von D_0 an, die durch Anwendung von E auf D_0 entstehen. Jede Menge $e_i D_0$ läßt sich also durch eine endliche Kette K_i mit D_0 verbinden. Eine solche Kette besteht aus Mengen $f_1 \dots f_k D_k$, $k = 0, \dots, m$, wobei die f_k Elemente von E und die D_k Zusammenhangskomponenten von D sind (die natürlich von i abhängen). Insbesondere ist $f_1 \dots f_m D_m = e_i D_0$; hieraus folgt die Existenz eines Elementes f aus E , das der Gleichung $e_i = f_1 \dots f_m f$ genügt. Jetzt wollen wir endlich die definierenden Relationen von H vollständig festlegen. Wir nehmen außer den lokalen Relationen

noch für jedes i die Relation $\bar{e}_i^{-1} \bar{f}_1 \dots \bar{f}_m \bar{f}$ hinzu.

Setzen wir jetzt $\bar{p}^1(D_k) \cap B = B_k$ für $k = 0, \dots, m$, so entspricht jeder Kette K_i in T eine Kette L_i in S , die aus den Mengen $s(\bar{f}_1) \dots s(\bar{f}_k) B_k$, $k = 0, \dots, m$ besteht. Die Vereinigungsmenge aller in den Ketten L_i vorkommenden Mengen wollen wir A nennen; offenbar ist A zusammenhängend. Nach Wahl der definierenden Relationen ist $s(\bar{e}_i) = s(\bar{f}_1) \dots s(\bar{f}_m) s(\bar{f})$; ferner gilt: $D_m = f D_0$. Auf Grund der Gleichheitsdefinition in S folgt hieraus die Beziehung $s(\bar{e}_i) B_0 = s(\bar{f}_1) \dots s(\bar{f}_m) B_m$, d.h. es gilt für jedes Element e aus E : $s(\bar{e}) A \cap A \neq \emptyset$.

Bis jetzt haben wir nur gezeigt, daß jede Zusammenhangskomponente von S ein Überlagerungsraum von T ist. Wegen des einfachen Zusammenhangs von T überlagert jede von ihnen T sogar schlicht. Wir interessieren uns nur für die Zusammenhangskomponente, die A enthält; sie heiße W . Ist $\bar{e}_r \dots \bar{e}_1$ eine Relation, so betrachten wir das Element $h = s(\bar{e}_r) \dots s(\bar{e}_1)$ in H und wenden es auf A an. Aus $s(\bar{e}) A \cap A \neq \emptyset$ für e aus E folgt für alle j mit $1 \leq j \leq r-1$: $s(\bar{e}_r) \dots s(\bar{e}_j) A \cap s(\bar{e}_r) \dots s(\bar{e}_{j+1}) A \neq \emptyset$ und hieraus, daß hA in W liegt. Da h im Kern von t liegt und da W den Raum T schlicht überlagert, ist h die Identität auf A . Ein Element aus dem Kern von t , das einen Punkt festläßt, ist aber selbst die Einheit, was man aus der Gleichheitsdefinition in S abliest. Also ist $h = 1$ und jede Relation aus R liegt schon in N . Damit ist Satz 2 bewiesen.

2. Beweis von Satz 3. Wir wählen ein Element A aus M , seine Fixgruppe heiße U . Sei K die Konstante aus Voraussetzung a), dann ist die Anzahl der Elemente B aus M mit $d(A, B) \leq K$ nach Voraussetzung b) endlich; wir nennen diese Elemente E_i , $i = 1, \dots, n$. Zu jedem E_i läßt sich wegen der Transitivität der Gruppe G auf M ein Element e_i aus G mit $e_i A = E_i$ finden. Die Menge $\{e_1, \dots, e_n\}$ bezeichnen wir mit $E(K)$. Nach Voraussetzung c) existiert außerdem ein endliches Erzeugendensystem E_U der Fixgruppe U von A . Wir behaupten nun, daß die Vereinigung E der Mengen $E(K)$ und E_U ein endliches Erzeugendensystem von G ist.

Ist ein beliebiges Element a aus G vorgegeben, so wenden wir ~~a~~auf A an, setzen $B = aA$ und führen den Beweis durch Induktion nach $d(A, B)$.

Ist $d(A, B) \leq K$, so gibt es ein Element e aus $E(K)$ mit $eA = B$, also liegt $e^{-1}a$ in der Fixgruppe U von A und wir haben für a die Darstellung $a = e u$ mit u aus U . Daraus folgt wegen der Erzeugbarkeit von U durch E_U die Behauptung.

Für den Induktionsschritt (wenn $d(A, B) > K$ ist) wenden wir Voraussetzung a) auf die Punkte A und $B = aA$ an. Diese zeigt, daß es einen Punkt C aus M mit $d(A, C) \leq K$ und $d(C, B) < d(A, B)$ gibt. Auf Grund der ersten Eigenschaft kann man ein Element f aus $E(K)$ mit $C = fA$ finden. Wir definieren dann den Punkt D durch $D = f^{-1}B$. Dann ist $D = f^{-1}a A$ und wir erhalten:
$$d(D, A) = d(f^{-1}B, A) = d(B, fA) = d(B, C) < d(B, A).$$

Wir können also die Induktionsvoraussetzung auf das Element $f^{-1}a$

anwenden und die Gleichung $a = f(f^{-1}a)$ liefert dann eine Darstellung von a durch Elemente aus E .

3. Beweis von Satz 4. Die Voraussetzungen von Satz 3 sind in denen von Satz 4 enthalten: die Gruppe G ist also endlich erzeugbar. Das im Beweis von Satz 3 beschriebene Erzeugenden - system $E = E(K) \cup E_U$ können wir so wählen, daß mit e auch e^{-1} in $E(K)$ liegt. Die von diesem System erzeugte freie Gruppe nennen wir F , den zum Homomorphismus von F auf G gehörigen Normalteiler der Relationen bezeichnen wir wieder mit R .

Wir werden analog zum Beweis von Satz 3 eine endliche Menge S von Relationen angeben und nachher zeigen, daß der von ihnen erzeugte Normalteiler N gleich R ist. Ehe wir S definieren, wollen wir aber den folgenden Hilfssatz beweisen (dabei bezeichnet A wieder den zur Definition von E benützten festen Punkt aus M).

Hilfssatz : Es seien die Voraussetzungen von Satz 4 erfüllt.

B und C seien zwei Punkte aus M und B gehe aus C durch Anwendung eines Produktes p von höchstens s Faktoren aus E hervor. Dann gibt es eine Punkt - folge $(B_0, \dots, B_k)$ in M mit folgenden Eigenschaften :

- 1) $B_0 = B, B_k = C$.
- 2) Zu jedem i mit $1 \leq i \leq k$ gibt es ein Element b_i aus E mit $B_i = b_i B_{i-1}$.
- 3) Es gilt: $d(B_1, A) \leq \max \{d(B, A), d(C, A)\}$.
- 4) Die Produkte $b_k \dots b_1 p$ sind für beliebige Punkte

B und C einer nur von s abhängigen endlichen Menge $R(s)$ von Relationen entnommen.

Beweis: a) Als erstes definieren wir einen Hilfspunkt D durch $D = pA$ und zeigen die Existenz einer Punktfolge $(D_0, \dots, D_l)$ mit $D_0 = A$, $D_l = D$ und den Abstandseigenschaften $d(D_i, D_{i+1}) \leq K$ für $0 \leq i \leq l-1$ sowie $d(D_i, B) \leq \max \{ d(A, B), d(D, B) \}$ für $0 \leq i \leq l$. Diese Folge konstruiert man, ausgehend von A, D, B , durch fortgesetzte Anwendung des zweiten Teils von Bedingung a) von Satz 4, solange die Voraussetzungen über die Abstände erfüllt sind. Ist schon $d(A, D) \leq K$, so ist nichts mehr zu konstruieren; ist aber $d(D, B) \leq K$, so nimmt man B als vorletzten Punkt in die Folge auf und gewinnt das Anfangsstück zwischen A und B nach dem ersten Teil von Bedingung 4a); wird einmal $d(D_1, B) \leq K$, so nimmt man wieder B als nächsten Punkt in die Folge auf und konstruiert das Reststück durch Anwendung des ersten Teils von 4a) auf B und D . Die Länge l der Folge ist in jedem Falle kleiner oder höchstens gleich $d(A, D) + K + 1$ und für $d(A, D)$ gilt (mit $p = a_s \dots a_1$) die Abschätzung:

$$\begin{aligned} d(A, D) = d(A, pA) &\leq d(A, a_s \dots a_2 A) + d(a_s \dots a_2 A, a_s \dots a_1 A) \\ &\leq d(A, a_s \dots a_3 A) + d(a_s \dots a_3 A, a_s \dots a_2 A) + \\ &\quad d(a_s \dots a_2 A, a_s \dots a_1 A) \leq \dots \leq s K. \end{aligned}$$

b) Zu jedem Punkt D_i wählen wir nun ein Element d_i aus G mit $d_i A = D_i$, insbesondere sei $d_0 = 1$. Aus $d(D_{i-1}, D_i) \leq K$ folgt dann: $d(d_{i-1}^{-1} d_i A, A) = d(d_i A, d_{i-1} A) = d(D_i, D_{i-1}) \leq K$. Setzen wir $b_i = d_i^{-1} d_{i-1}$ für $i = 1, \dots, l$, so besagt die obige

Ungleichung einfach $d(b_i^{-1}A, A) \leq K$. Wenn wir für $i = 1, 2, \dots, l$ nacheinander noch d_i durch $d_i u_i$ mit geeignetem u_i aus U ersetzen, so können wir sogar erreichen, daß die Elemente b_i^{-1} in E liegen; nach Konstruktion von E gilt dann dasselbe auch von b_i . Betrachten wir nun das Produkt $b_1 \dots b_l p$. Es ist

$$b_1 \dots b_l p = (d_1^{-1} d_{l-1}) (d_{l-1}^{-1} d_{l-2}) \dots (d_2^{-1} d_1) (d_1^{-1} d_0) p = d_1^{-1} p;$$

folglich läßt dieses Produkt den Punkt A fest, denn nach unseren Definitionen ist $d_1 A = D_1 = D = pA$.

c) Mit Hilfe der in b) konstruierten Elemente b_i definieren wir nun rekursiv die Punktfolge $(B_0, \dots, B_l)$ durch: $B_0 = B$ und $B_i = b_i B_{i-1}$ für $1 \leq i \leq l$.

Diese Folge hat bereits die gewünschten Eigenschaften 2 und 3.

Für Eigenschaft 3 sieht man das so ein: Es ist $d(A, C) = d(pA, pC) = d(D, B)$ und $B_i = b_i B_{i-1} = b_1 \dots b_i B = d_i^{-1} B$. Dann folgt aus $d(D_i, B) \leq \max \{d(A, B), d(D, B)\}$ die Beziehung

$$d(B_i, A) = d(d_i^{-1} B, A) = d(B, d_i A) = d(B, D_i) \\ \leq \max \{d(B, A), d(B, D)\} = \max \{d(B, A), d(C, A)\}.$$

d) Die Folge $(B_0, \dots, B_l)$ aus c) braucht noch nicht zum Punkt C zu führen (das hieße $B_l = C$), denn das Produkt $b_1 \dots b_l p$ läßt zwar A fest, ist aber nicht notwendig gleich 1. Bei vorgegebenem s und beliebigen Punkten B und C bestehen alle diese Produkte $b_1 \dots b_l p$ nach der Abschätzung in a) aus höchstens $sK + K + 1 + s$ Faktoren aus E . Da sie A festlassen, entsteht aus jedem von ihnen durch Multiplikation von links mit einem geeigneten Element u aus U , also einem Produkt von Elementen

aus E_U , eine Relation. Die so entstehende endliche Menge von Relationen nennen wir $R(s)$.

Wir schreiben das zum Produkt $b_1 \dots b_1 p$ gehörige Element u als Produkt von Faktoren aus E_U in der Form $u = b_k \dots b_{l+1}$. Dann definieren wir das Reststück der gesuchten Folge $(B_0, \dots, B_k)$ durch: $B_{l+1} = b_{l+1} B_l, \dots, B_k = b_k B_{k-1}$. Jetzt ist $B_k = C$, denn es gilt: $B_k = b_k \dots b_1 B = b_k \dots b_1 p C = C$.

Damit haben wir für den Beweis des Hilfssatzes nur noch nachzurechnen, daß auch das Reststück $(B_{l+1}, \dots, B_k)$ die geforderten Abstandseigenschaften hat:

$$\begin{aligned} d(B_l, A) &= d(b_l B_{l-1}, A) = d(B_{l-1}, b_l^{-1} A) = d(B_{l-1}, A) = \dots = \\ &= d(B_1, A) \leq \max \{d(B, A), d(C, A)\}. \end{aligned}$$

Genau wie im Beweis des Hilfssatzes können wir zu jedem Produkt q von höchstens drei Faktoren aus E , das den Punkt A festläßt, ein Element u aus U wählen, so daß uq eine Relation ist. Die hierdurch entstehende Relationenmenge nennen wir R_3 . Nach Voraussetzung 4c) existiert eine endliche Menge R_U von definierenden Relationen von U ; außerdem sei $R(3)$ die nach dem Hilfssatz zu $s = 3$ gehörige Relationenmenge. Wir bezeichnen die Vereinigungsmenge von R_U , R_3 und $R(3)$ mit S und werden nun beweisen, daß der von S erzeugte Normalteiler N gleich R ist.

Jedes Element der freien Gruppe F besitzt eine eindeutige gekürzte Normalform. Der Normalform einer beliebigen Relation ordnen wir eine endliche Punktfolge in M zu, bei der Anfangs- und Endpunkt zusammenfällt; die Zuordnung definieren wir so :

Ist $r = a_n \dots a_1$ die Normalform einer Relation, dann entsteht die zugehörige Punktfolge $\bar{r} = (A_0, \dots, A_n)$ dadurch, daß man die aufeinanderfolgenden Teilprodukte $a_p \dots a_1$ ($p = 0, \dots, n$) von r auf den festen Punkt A anwendet, also $A_p = a_p \dots a_1 A$ setzt.

Der folgende Beweis hat einen „anschaulichen“ Grundgedanken: Man ziehe den soeben einer Relation zugeordneten „geschlossenen Weg“ mit Hilfe der Relationen aus N schrittweise zusammen. Wir definieren daher für eine Punktfolge $\bar{r} = (A=A_0, A_1, \dots, A_n=A)$ den Abstand von A durch $D(\bar{r}) = \max_{0 \leq i \leq n} d(A_i, A)$, und führen einen Induktionsbeweis nach $D(\bar{r})$. Genauer gesagt, machen wir folgendes: Für eine Relation r mit $D(\bar{r}) \leq K$ zeigen wir durch sukzessive Multiplikation von r mit Elementen aus N , daß $r \bmod N$ kongruent einer Relation aus N ist, also selbst in N liegt. Zu einer Relation r mit $D(\bar{r}) > K$ konstruieren wir eine Relation r' , die $\bmod N$ zu r kongruent ist und für die gilt: $D(\bar{r}') < D(\bar{r})$.

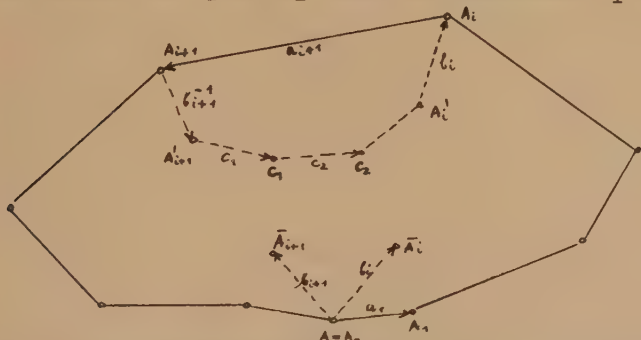
Zunächst sei also eine Relation r mit $D(\bar{r}) \leq K$ vorgelegt; die Normalform sei $a_n \dots a_1$, der zugehörige Weg $\bar{r} = (A=A_0, \dots, A_i, \dots, A_n=A)$. Wegen $D(\bar{r}) \leq K$ ist für jedes i ($0 \leq i \leq n$) auch $d(A_i, A) \leq K$, so daß man nach Konstruktion von E zu jedem Punkt A_i ein Element b_i aus E mit $b_i A = A_i$ finden kann. Die Produkte $b_i^{-1} a_{i+1}^{-1} b_{i+1}$ ($0 \leq i \leq n-1$) lassen den Punkt A fest. Nach Definition von R_3 gehört zu jedem von ihnen ein Element u_i aus U , so daß das Produkt $s_i = u_i b_i^{-1} a_{i+1}^{-1} b_{i+1}$ in R_3 und damit in S liegt. Dann ist das konjugierte Produkt

$t_i = a_{i+1}^{-1} b_{i+1} u_i b_i^{-1}$ Element von N . Das Produkt t_i in das Produkt $r = a_n \dots a_1$ zwischen die Faktoren a_{i+1} und a_i einschreiben, bedeutet r mit einem geeigneten Konjugierten von t_i , also mit einem Element von N multiplizieren. Dabei geht r in eine zu $r \bmod N$ kongruente Relation über. Die Durchführung dieses Prozesses für alle i liefert schließlich eine Relation

$r' = b_n u_n \dots u_0 b_0^{-1}$, deren Faktoren alle in U liegen (denn wegen $A_0 = A = A_n$ sind auch b_0 und b_n Elemente von U) und die $\bmod N$ zu r kongruent ist. (Es ist zu bemerken, daß die u_i für ein Produkt von Faktoren aus E_U stehen.) Nach Definition von R_U liegt aber dann r' in dem von R_U in F erzeugten Normalteiler, also erst recht in N .

Für eine Relation r mit $D(\bar{r}) > K$ haben wir nun den Reduktionsschritt vorzunehmen. Zu diesem Zweck konstruieren wir zu jedem Punkt A_i von $\bar{r}$, der den maximalen Abstand $D(\bar{r})$ von A hat, einen Punkt A'_i aus M , der aus A_i durch Anwendung eines Elementes aus $E(K)$ ($\subset E$) hervorgeht und dessen Abstand von A kleiner ist als der von A_i und A . Die Anwendung des ersten Teils von Voraussetzung 4a) auf die Punkte A und A_i liefert zunächst einen Punkt $\bar{A}_i$ mit den Eigenschaften $d(\bar{A}_i, A) \leq K$ und $d(\bar{A}_i, A_i) < d(A, A_i)$; aus der ersten folgt die Existenz eines Elementes b_i aus $E(K)$ mit $b_i A = \bar{A}_i$. Dann liegt nach Definition von $E(K)$ auch b_i^{-1} in $E(K)$; wir können daher A'_i durch $A'_i = b_i^{-1} A_i$ definieren, tatsächlich hat dann A'_i auch die gewünschte Abstandseigenschaft: $d(A'_i, A) = d(b_i^{-1} A_i, A) = d(A_i, b_i A) = d(A_i, \bar{A}_i) < d(A_i, A) = D(\bar{r})$.

Für Punkte A_i von $\bar{r}$, deren Abstand von A kleiner ist als $D(\bar{r})$, definieren wir A'_i und b_i durch die Festsetzung $A'_i = A_i$, $b_i = 1$.



Betrachten wir nun ein Punktepaar A_i, A_{i+1} von $\bar{r}$, bei dem wenigstens ein Punkt den maximalen Abstand $D(\bar{r})$ von A hat. Auf das zugeordnete Paar A'_i, A'_{i+1} können wir nun unseren Hilfssatz anwenden, denn A'_i geht aus A'_{i+1} durch Anwendung eines Produktes von drei Faktoren aus E hervor: $A'_i = b_i^{-1} a_{i+1}^{-1} b_{i+1} A'_{i+1}$.

Es gibt also eine Punktfolge $(C_0, \dots, C_k)$ mit $C_0 = A'_i$ und $C_k = A'_{i+1}$, die die Abstanseigenschaft

$$d(C_j, A) \leq \max \{ d(A'_i, A), d(A'_{i+1}, A) \} \quad \text{für } 0 \leq j \leq k-1 \text{ besitzt.}$$

Außerdem existieren Elemente c_j aus E mit $C_j = c_j C_{j-1}$

$(1 \leq j \leq k)$ und das Produkt $c_k \dots c_1 b_i^{-1} a_{i+1}^{-1} b_{i+1}$ liegt in $R(3)$.

Das Produkt $v_i = a_{i+1}^{-1} b_{i+1} c_k \dots c_1 b_i^{-1}$ liegt dann in N . Einschleiben des Produktes v_i in die Relation r zwischen a_{i+1} und a_i bedeutet wieder Multiplikation von r mit einem geeigneten Konjugierten von v_i , also Übergang von r zu einer mod N kongruenten Relation. Führen wir diesen Prozeß für alle in Frage kommenden Punktepaare von $\bar{r}$ durch, so bekommen wir schließlich

eine Relation r' , die mod N zu r kongruent ist und deren zugeordneter Weg $\bar{r}'$ einen Abstand $D(\bar{r}') < D(\bar{r})$ hat, denn die b_i heben sich alle heraus und folglich kommen in $\bar{r}'$ nur noch die Punkte A_i von $\bar{r}$ mit $d(A_i, A) < D(\bar{r})$ und die Punkte C vor, die die Eigenschaft $d(C, A) < D(\bar{r})$ ebenfalls haben. Damit ist der Beweis von Satz 4 vollständig.

Bemerkung: Bei der Anwendung der Sätze 3 und 4 kommt es vor, daß man die Konstante K von Satz 4 größer wählen muß als die Konstante K in Satz 3. Vergrößerung von K bedeutet im allgemeinen eine Vergrößerung des Erzeugendensystems. Man kann aber die Gruppe G dann auch durch endlich viele Relationen zwischen den Erzeugenden des kleineren Systems definieren, denn es gilt der Satz (vgl.(5), Seite 81): Wenn die Gruppe G durch ein endliches System von Erzeugenden, die durch endlich viele definierende Relationen verknüpft sind, gegeben ist, dann kann die Gruppe auch in jedem anderen endlichen System von Erzeugenden durch endlich viele Relationen definiert werden.

Abschnitt II:

LINEARE UND ORTHOGONALE EINHEITENGRUPPEN.

In diesem Abschnitt wollen wir die allgemeinen Sätze des vorigen Abschnitts auf die gewöhnlichen und verallgemeinerten Einheitengruppen der allgemeinen und speziellen linearen Gruppe sowie der orthogonalen Gruppen über dem Körper der rationalen Zahlen anwenden.

1. Allgemeine lineare Gruppe. Die Gruppe aller nicht singulären n -reihigen Matrizen mit Elementen aus dem Körper Q der rationalen Zahlen nennt man die allgemeine lineare Gruppe über Q und bezeichnet sie mit $GL_n(Q)$. Unter ihrer Einheitsgruppe versteht man diejenige Untergruppe, deren Matrizen Elemente aus dem Ring Z der ganzen Zahlen und Determinante $+1$ oder -1 haben; wir bezeichnen sie mit $GL_n(Z)$. Ist S eine endliche Menge von Primzahlen, so bilden die Elemente aus Q , bei denen in der Primfaktorzerlegung des Nenners nur Potenzen von Primzahlen aus S auftreten, einen Ring Z_S . Als verallgemeinerte Einheitengruppe bezüglich S bezeichnen wir die Gruppe $GL_n(Z_S)$ aller nicht singulären n -reihigen Matrizen mit Elementen aus Z_S , deren Determinante eine relative Einheit bezüglich S ist (d.h. Zähler und Nenner der Determinante sind prim zu allen nicht in S gelegenen Primzahlen).

Mit diesen Bezeichnungen gilt dann der folgende Satz:

Satz 5. Die Gruppen $GL_n(Z)$ und $GL_n(Z_S)$ können durch endlich viele Elemente erzeugt und durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden.

Beweis: Die endliche Erzeugbarkeit von $GL_n(Z)$ ist ein Resultat von Minkowski (siehe (6), S.220 oder (7), Band 2, S.53). Wir wollen hier kurz den Grundgedanken eines von Siegel (in (11), S.212) angegebenen Beweises skizzieren. Man kann ihn auffassen als Anwendung von Satz 1 auf die Faktorgruppe $GL_n'(Z)$ von $GL_n(Z)$ nach der Untergruppe $\{e, -e\}$ (e ist die n -reihige Einheitsmatrix). Tatsächlich hat Siegel etwas mehr bewiesen. Sagt man, daß die Gruppe G bezüglich des topologischen Raumes T den Fundamentalbereich F besitzt, wenn folgendes erfüllt ist:

- a) Zu jedem Punkt P von T existiert höchstens ein Element a aus G , so daß aP in F liegt.
 - b) Zu jedem Punkt P von T existiert mindestens ein Element a aus G , so daß aP in $\bar{F}$ liegt ($\bar{F}$ = abgeschlossene Hülle von F)
- so hat Siegel nämlich gezeigt, daß $GL_n'(Z)$ bezüglich des Raumes T der n -reihigen positiven symmetrischen Matrizen über dem Körper R der reellen Zahlen eine von endlich vielen Hyperebenen begrenzte konvexe Ecke E als Fundamentalbereich besitzt. Dabei hat $\bar{E}$ nur mit den abgeschlossenen Hüllen von endlich vielen Bildern E_i von E Punkte gemeinsam. Dann gibt es in T aber auch eine offene Menge D mit den in Satz 1 verlangten Eigenschaften: man nehme z.B. den offenen Kern der Vereinigungsmenge von E und den endlich vielen E_i . T ist ein konvexer Raum, also auch ein-

fach zusammenhängend. Daraus ergibt sich sofort die Anwendbarkeit von Satz 2 auf $GL'_n(Z)$. Aus dem Resultat für $GL'_n(Z)$ können wir nun die Behauptung für $GL_n(Z)$ ableiten.

Die Erzeugenden der Gruppe $GL'_n(Z)$ sind Nebenklassen der Gruppe $\{e, -e\}$ in $GL_n(Z)$. Wir wählen aus jeder von ihnen einen Vertreter und nennen ihre Gesamtheit E' . Nehmen wir zu E' noch das Element $-e$ hinzu, so erhalten wir offenbar ein Erzeugendensystem der Gruppe $GL_n(Z)$.

Das System der definierenden Relationen von $GL'_n(Z)$ heiße S . Zu jeder von ihnen bilden wir das entsprechende Produkt mit Faktoren aus E' . Dieses Produkt ist gleich e oder $-e$; im zweiten Fall fügen wir $-e$ als Faktor dazu und gewinnen so eine Menge R' von Relationen von $GL_n(Z)$. $-e$ ist mit jedem Element vertauschbar, also ist jeder Kommutator von $-e$ und einem Element aus E' eine Relation; die Menge dieser Relationen bezeichnen wir mit R'' . Nehmen wir zu R' und R'' noch die Relation $r = (-e)(-e)$ hinzu, so erhalten wir eine Menge R , von der wir nun zeigen, daß sie ein System definierender Relationen von $GL_n(Z)$ bildet.

Es sei nun eine beliebige Relation vorgelegt. Durch Multiplikation mit Konjugierten von Elementen aus R'' sowie mit r erhalten wir zunächst einen Ausdruck der Form $(-e)s$ oder s , wobei s nur Faktoren aus E' enthält. Man kann s als Relation von $GL'_n(Z)$ auffassen. Als solche besitzt es eine Darstellung durch das System S . Zu dieser bilden wir nun den entsprechenden Ausdruck mit Relationen aus R' . Die dabei hereinkommenden Faktoren $-e$ bringen wir genau wie vorher zum Verschwinden, vielleicht mit Ausnahme eines

Faktors $-e$ am Anfang. Das so entstandene Produkt ist dann gleich $(-e) s$ oder s . Insgesamt gewinnt man eine Darstellung der ursprünglich gegebenen Relation durch das endliche System R .

Den Beweis für die Gruppen $GL_n(Z_S)$ führen wir durch vollständige Induktion nach der Anzahl m der Elemente von S . Da man die Gruppe $GL_n(Z)$ als Gruppe $GL_n(Z_S)$ mit $m = 0$ auffassen kann, ist der Induktionsanfang bereits erledigt. Setzen wir $S = \{p_1, \dots, p_m\}$ und $R = \{p_1, \dots, p_{m-1}\}$, so besteht der Induktionsschritt darin, aus der Richtigkeit der Behauptung für $GL_n(Z_R)$ die für $GL_n(Z_S)$ zu folgern; hierzu verwenden wir die Sätze 3 und 4.

Zur Abkürzung setzen wir $p_m = p$ und bezeichnen mit Q_p den Körper der p -adischen Zahlen, mit Z_p den Ring der ganzen p -adischen Zahlen und mit Q^n bzw. Q_p^n den n -dimensionalen Vektorraum über Q bzw. Q_p . Unter einem Gitter in Q^n bzw. Q_p^n verstehen wir einen endlich erzeugten Z - bzw. Z_p -Modul, der n linear unabhängige Vektoren enthält. Die Matrizen aus $GL_n(Z_S)$ fassen wir von nun an immer als Darstellungen linearer Abbildungen der Vektorräume Q^n bzw. Q_p^n auf, bezogen auf die von den Einheitsvektoren dieser Räume gebildete Basis. Die von diesen Vektoren in Q^n bzw. in Q_p^n aufgespannten Gitter nennen wir $\bar{A}$ bzw. A ($A = \bar{A} \otimes_{\mathbb{Z}} Z_p$ ist die perfekte Hülle von $\bar{A}$ bezüglich p).

Nun können wir die Menge M definieren, auf der die Gruppe $GL_n(Z_S)$ transitiv operiert: es sei die Menge aller Gitter in Q_p^n ,

die aus dem Gitter A durch Anwendung eines Elementes aus $GL_n(Z_S)$ entstehen. In M läßt sich ein Abstand erklären durch die Definition: $d(B,C) = \min s$ mit $p^s B \subseteq C$ und $p^s C \subseteq B$.

Für diesen Abstand gilt ersichtlich die Dreiecksungleichung; außerdem ist er gegenüber Anwendung von Elementen aus $GL_n(Z_S)$ invariant, da diese lineare Abbildungen darstellen.

Den Nachweis der Voraussetzungen der Sätze 3 und 4 können wir zusammen führen. Zunächst ist klar, daß die Fixgruppe des Gitters A gerade die Gruppe $GL_n(Z_R)$ ist, denn A ist Z_p -Modul.

Also sind nach Induktionsannahme die Bedingungen c) erfüllt.

Zweitens ist leicht zu sehen, daß es zu festem Gitter B aus M und beliebiger Konstante L nur endlich viele Gitter C aus M (sogar aus Q_p^n) gibt, die der Bedingung $p^L B \subseteq C \subseteq p^{-L} B$ genügen. Etwas mehr Mühe machen die Voraussetzungen a). Aus dem Elementarteilersatz folgt, daß es zu zwei beliebigen Gittern B und C aus M Basen $[i_1, \dots, i_n]$ von B und $[j_1, \dots, j_n]$ von C gibt mit $j_1 = p^{a_1} i_1$. Wir definieren das Gitter D durch Angabe der folgenden Basis: $[k_1, \dots, k_n]$ mit $k_1 = p^{b_1} i_1$ und $b_1 = \text{signum } a_1$. Dann ist $d(B,D) = 1$ und $d(C,D) < d(B,C)$, falls $B \neq C$ ist. Ist

E ein weiteres Gitter aus M mit $E \neq B$ und $E \neq C$, so überlegt man sich an Hand der angegebenen Basen leicht, daß $d(D,E) \leq \max \{d(B,E), d(C,E)\}$ ist. Wir können also die Konstanten K in den Bedingungen a) gleich 1 wählen, wenn es uns gelingt zu zeigen, daß D in M liegt; d.h. wir haben noch die Existenz eines Elementes b aus $GL_n(Z_S)$ mit $bA = D$ zu beweisen. (Diese folgt noch nicht aus der angegebenen Konstruktion von D,

denn wir haben ja die lineare Abbildung b auf die von den Einheitsvektoren gebildete Basis zu beziehen). Wir benützen dazu folgende Hilfskonstruktion (vgl. (1), S.75): Ist $\bar{A}_q = \bar{A} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ die q -adische Hülle von $\bar{A}$ (insbesondere also $\bar{A}_p = A$), so gilt: $\bar{A} = \bigcap_q (\bar{A}_q \cap \mathbb{Q}^n)$ (dabei ist der Durchschnitt über alle Primzahlen q erstreckt). Gibt man umgekehrt Gitter $\bar{B}_q$ in $\mathbb{Q}_q^n$ so vor, daß für fast alle q $\bar{B}_q = \bar{A}_q$ ist, so ist die durch $\bar{B} = \bigcap_q (\bar{B}_q \cap \mathbb{Q}^n)$ definierte Menge ein Gitter in $\mathbb{Q}^n$ und es gilt die Beziehung $\bar{B} \otimes_{\mathbb{Z}} \mathbb{Z}_q = \bar{B}_q$. Auf diese Weise können wir nun zu D ein Gitter $\bar{D}$ in $\mathbb{Q}^n$ definieren durch $\bar{D} = \bigcap_{q \neq p} (\bar{A}_q \cap \mathbb{Q}^n) \cap D$. Da $\mathbb{Z}$ Hauptidealring ist, besitzen $\bar{A}$ und $\bar{D}$ Basen, folglich gibt es eine lineare Transformation c von $\mathbb{Q}^n$, die $\bar{A}$ in $\bar{D}$ überführt. c transformiert dann auch die perfekten Hüllen, d.h. es gilt: $c\bar{A}_q = \bar{D}_q$ für alle $q \neq p$ und $cA = D$. Aus diesen Gleichungen folgt wegen $\bar{A}_q = \bar{D}_q$ für $q \neq p$, daß die Matrixelemente von c (in der Darstellung bezüglich der Einheitsvektoren) in $\mathbb{Z}_{\{p\}}$, also erst recht in $\mathbb{Z}_S$ liegen und daß keine Primzahl $q \neq p$ die Determinante von c teilt; dann ist die Determinante aber eine relative Einheit bezüglich S .

2. Spezielle lineare Gruppe. Unter der speziellen linearen Gruppe über $\mathbb{Q}$ versteht man die Gruppe $SL_n(\mathbb{Q})$ aller n -reihigen Matrizen mit Elementen aus $\mathbb{Q}$ und Determinante $+1$. Ihre Einheitengruppe $SL_n(\mathbb{Z})$ ist diejenige Untergruppe, deren Matrixelemente ganzrational sind. Die verallgemeinerte Einheitsengruppe $SL_n(\mathbb{Z}_S)$ (bezüglich der endlichen Primzahlmenge S)

definieren wir als die Gruppe aller n -reihigen Matrizen mit Elementen aus Z_S und Determinante 1. Dann gilt der

Satz 6. Die Gruppen $SL_n(Z)$ und $SL_n(Z_S)$ können durch endlich viele Elemente erzeugt und durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden.

Beweis: Die Aussage über die Gruppe $SL_n(Z)$ läßt sich aus der entsprechenden für $GL_n(Z)$ ableiten, denn $SL_n(Z)$ ist Normalteiler in $GL_n(Z)$ vom Index 2. Ist e_0 ein Element aus $GL_n(Z)$ mit Determinante -1 , so kann man e_0 zu einem Erzeugendensystem $(e_0, e_1, \dots, e_n)$ von $GL_n(Z)$ ergänzen, bei dem die Elemente $e_1, \dots, e_n$ in $SL_n(Z)$ liegen. Dann bilden die Elemente e_1 und $d_i = e_0^{-1} e_1 e_0$ für $i = 1, \dots, n$ ein Erzeugendensystem von $SL_n(Z)$. Stellt man nämlich ein Element aus $SL_n(Z)$ mit Hilfe des Erzeugendensystems $(e_0, \dots, e_n)$ dar, so kann man e_0 durch Einführung der Elemente d_i eliminieren. Genau so geht man bei den Relationen vor und findet, daß $SL_n(Z)$ durch endlich viele Relationen zwischen seinen Erzeugenden definiert werden kann.

Um die Behauptung für die Gruppen $SL_n(Z_S)$ zu beweisen, brauchen wir den in 1 geführten Beweis für $GL_n(Z_S)$ nur geringfügig abzuändern; die Bezeichnungen werden übernommen. Man definiert die Menge M jetzt, indem man $SL_n(Z_S)$ auf das Gitter A anwendet und versieht M mit derselben Metrik wie in 1. Die Fixgruppe von A ist $SL_n(Z_R)$, auf sie ist also wieder die Induktionsvoraussetzung anwendbar.

Nur bei der Konstruktion des Zwischengitters D hat man auf die

Einschränkung der Determinante zu achten. Seien $[i_1, \dots, i_n]$ und $[j_1, \dots, j_n]$ wieder die Basen zweier Gitter B und C aus M mit $j_1 = p^{a_1} i_1$; wir ordnen sie jetzt so, daß $a_{1+1} \leq a_1$ ist. Ist $B \neq C$, so gibt es positive und negative a_1 , denn da B und C aus M sind, existiert ein Element a aus $SL_n(Z_S)$ mit $aB = C$ und da die Determinante von a gleich 1 ist, folgt daraus, daß $\sum_{i=1}^n a_i = 0$ ist. Wir nehmen an, daß es unter den Exponenten a_i r positive und s negative gibt und daß $r \geq s$ ist (der Fall $s \geq r$ wird analog behandelt). Wir definieren nun das Gitter D durch die Basis $[p i_1, \dots, p i_s, \dots, p^{-1} i_{n-s+1}, \dots, p^{-1} i_n]$. Hieraus folgen dann wieder die Aussagen über die Abstände. Genau wie in 1 konstruieren wir eine lineare Transformation c mit Koeffizienten in Z_S , die A in D überführt. Zusätzlich folgt jetzt auf Grund der Konstruktion von D, daß die Determinante von c nicht nur für alle Primzahlen $q \neq p$ sondern auch für $q = p$ eine Einheit von Q_q ist; dann muß sie +1 oder -1 sein. Dann kann man aber auch ein Element b aus $SL_n(Z_S)$ finden mit $bA = D$. Damit sind wieder alle Bedingungen der Sätze 3 und 4 nachgewiesen.

3. Orthogonale Gruppe. Mit s bezeichnen wir eine nicht ausgeartete quadratische Form über dem Körper Q der rationalen Zahlen und gleichzeitig auch ihre Koeffizientenmatrix. Die Gesamtheit der Matrizen x aus $GL_n(Q)$, die der Gleichung $x^T s x = s$ genügen (x^T = transponierte Matrix von x), heißt die zu s gehörige orthogonale Gruppe $O_n(Q, s)$. Als Einheitengruppe von s bezeichnet man die Untergruppe von $O_n(Q, s)$, deren Matricelemente

ganzrational sind, wir nennen sie $O_n(Z, s)$. Zu einer endlichen Menge S von Primzahlen definieren wir die verallgemeinerte Einheitengruppe $O_n(Z_S, s)$: es sei die Untergruppe von $O_n(Q, s)$, deren Matrixelemente aus dem Ring Z_S stammen.

Satz 7. Die Gruppen $O_n(Z, s)$ und $O_n(Z_S, s)$ können durch endlich viele Elemente erzeugt und durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden.

Beweis: Für definite quadratische Formen ist $O_n(Z, s)$ sogar endlich (siehe etwa (1), Satz 16.1); für indefinite quadratische Formen wurde die endliche Erzeugbarkeit von $O_n(Z, s)$ von Siegel bewiesen (siehe (11), S.224). Sein Beweis benützt im Prinzip wieder Satz 1. Als Raum, auf dem $O_n(Z, s)$ operiert, wird eine Mannigfaltigkeit W im Raum T der n -reihigen positiven symmetrischen reellen Matrizen verwendet, die durch die Gleichung $h s^{-1} h = s$ definiert wird. $O_n(Z, s)$ besitzt bezüglich W einen Fundamentalbereich F , dessen abgeschlossene Hülle $\bar{F}$ nur mit endlich vielen ihrer Bildbereiche Punkte gemeinsam hat (zur Konstruktion von F wird der in 1 beschriebene Fundamentalbereich E von $GL_n(Z)$ in T benützt, insbesondere wird F von Hyper-ebenen aus W ausgeschnitten). Daß W zusammenhängend ist, beweist Siegel durch Angabe einer Parameterdarstellung.

Mit ihrer Hilfe läßt sich auch zeigen, daß W sogar einfach zusammenhängend ist; wir führen dies aus, um auch Satz 2 anwenden zu können. Die Gleichung für W lautete: $h s^{-1} h = s$. s kann man reell auf Diagonalgestalt transformieren: $c^T s c = d$. Wenn h

Lösung von $hs^{-1}h = s$ ist, dann genügt $h' = c^T h c$ der Gleichung $h'd^{-1}h' = d$; der Übergang $h \rightarrow h'$ stellt eine umkehrbare lineare Abbildung von W in T dar. Wir betrachten jetzt die durch $hd^{-1}h = d$ definierte Mannigfaltigkeit W' ; für diese lautet die erwähnte Parameterdarstellung (siehe (11), S.226 bzw. 229):

$$h = 2z - d, \quad z = \begin{pmatrix} t^{-1} & t^{-1}y^T \\ yt^{-1} & yt^{-1}y^T \end{pmatrix}, \quad t = e - y^T y > 0 \quad (\text{d.h.}$$

positiv definit); dabei ist, wenn $(l, n-l)$ die Signatur von s bezeichnet, y eine $(n-l, n)$ -Matrix und e die l -reihige Einheitsmatrix. Man hat damit eine umkehrbar eindeutige und in beiden Richtungen rationale (also topologische) Abbildung von W' auf den Teil V des y -Raums, in dem $t = e - y^T y$ positiv ist. Es genügt also zu zeigen, daß V einfach zusammenhängend ist; wir beweisen, daß V eine konvexe Menge ist. Zu diesem Zweck führen wir in V eine Metrik ein und zwar durch Vorgabe der symmetrischen Bilinearform $(y_1, y_2) = x^T y_1^T y_2 x$ mit einem festen Spaltenvektor $x \neq 0$. Die zugehörige Matrix ist die l -fache direkte Summe von $x \cdot x^T$, die hierdurch definierte quadratische Form ist also halbpositiv. Daraus folgt die Gültigkeit der Cauchy-

$$\text{Schwarzschen Ungleichung: } (y_1, y_2) \leq \sqrt{(y_1, y_1)} \sqrt{(y_2, y_2)}.$$

Setzen wir $\bar{y} = ky_1 + (1-k)y_2$ mit reellem k zwischen 0 und 1, so erhält man

$$\begin{aligned} x^T \bar{y}^T \bar{y} x &= \sqrt{(\bar{y}, \bar{y})^2} \leq (k \sqrt{(y_1, y_1)} + (1-k) \sqrt{(y_2, y_2)})^2 \\ &\leq \max_{p=1,2} \sqrt{(y_p, y_p)^2} = \max_{p=1,2} x^T y_p^T y_p x < x^T x \end{aligned}$$

(letzteres wegen $t = e - y^T y > 0$)

Da x beliebig war, besagt dies gerade, daß V konvex ist.

Beim Beweis für die Gruppen $O_n(Z_S, s)$ gehen wir genauso wie bei den Gruppen $GL_n(Z_S)$ vor, nur die heranzuziehenden Hilfs-sätze werden diesmal etwas komplizierter. Wir führen also wieder einen Induktionsbeweis nach der Anzahl der Elemente von S ; dabei ist der Induktionsanfang durch den Beweis für $O_n(Z, s)$ bereits erledigt und für den Induktionsschritt werden wieder die Sätze 3 und 4 herangezogen.

Zunächst sind einige Definitionen und Begriffe einzuführen (für das Folgende vergleiche man stets das Buch von Eichler(1)). Durch die Vorgabe der quadratischen Form s wird der Vektorraum Q^n zu einem halbeinfachen metrischen Raum. Das zu s gehörige Skalarprodukt zweier Vektoren x und y bezeichnen wir einfach mit xy . Ein metrischer Vektorraum heißt anisotrop, wenn für keinen Vektor $x \neq 0$ $xx = 0$ ist. Ist A ein Gitter, dann nennt man den g.g.T. aller Ausdrücke $\frac{1}{2} x^2 = \frac{1}{2} xx$ mit x aus A die Norm von A : $n(A)$; der mit $n(A)^{-n}$ multiplizierte g.g.T. aller Determinanten von Skalarproduktmatrizen von n Vektoren aus A heißt die reduzierte Determinante von A : $\mathcal{D}(A)$. Ein Gitter heißt maximal, wenn es in keinem anderen Gitter gleicher Norm erhalten ist und schließlich werden zwei Gitter aus einem Raum K^n isomorph genannt, wenn sie durch ein Element aus $O_n(K, s)$ ineinander übergeführt werden können. Wir setzen wieder $S = \{p_1, \dots, p_m\}$, $R = \{p_1, \dots, p_{m-1}\}$ sowie $p = p_m$. Dann ist nach Induktionsvoraussetzung die Behauptung für $O_n(Z_R, s)$ bewiesen. Das von den Einheitsvektoren in Q^n aufgespannte Gitter sei $\bar{A}$, seine p -adische Hülle A ($= \bar{A} \otimes_{\mathbb{Z}} \mathbb{Z}_p$).

Wir nehmen zunächst an, daß A maximal ist. Als Menge N , auf die wir die Sätze 3 und 4 anwenden wollen, führen wir die Menge aller Gitter in Q_p^n ein, die aus A durch Anwendung eines Elementes von $O_n(Z_{S,s})$ entstehen. Lassen wir stattdessen sogar Elemente von $GL_n(Z_S)$ zu, so erhalten wir eine Menge von Gittern, die wir bereits in 1 mit M bezeichneten. In M haben wir einen Abstand definiert, der die gewünschten Eigenschaften hatte. Da N Teilmenge von M ist, können wir diese Definition übernehmen, dann erfüllt N die Voraussetzungen 3b) und 4b). Da die Fixgruppe von A gerade wieder $O_n(Z_{R,s})$ ist, gelten nach Induktionsannahme die Bedingungen 3c) und 4c).

Wir geben uns nun zwei beliebige Gitter B und C aus N vor ($B = C$); nach Konstruktion von N sind sie maximal. Dann gibt es (nach Satz 9.5 in (1)) Basen x_i und y_i von B bzw. C mit $y_i = p^{t_i} x_i$, die außerdem folgende Eigenschaften haben: Die Matrizen $(x_i x_j)$ und $(y_i y_j)$ haben die Gestalt

$$\begin{pmatrix} b_0 & & & & \\ & \begin{array}{|c|c|c|c|} \hline o & p^r & & \\ \hline p^r & o & & \\ \hline & & o & p^r \\ \hline o & & p^r & o \\ \hline \end{array} & & o \\ & & & & \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} c_0 & & & & \\ & \begin{array}{|c|c|c|c|} \hline o & p^s & & \\ \hline p^s & o & & \\ \hline & & o & p^s \\ \hline o & & p^s & o \\ \hline \end{array} & & o \\ & & & & \end{pmatrix}$$

dabei ist $p^r = n(B)$ und $p^s = n(C)$, b_0 und c_0 sind die Matrizen zweier maximaler Gitter B_0 und C_0 in einem anisotropen Teilraum $(Q_p^n)_0$ von Q_p^n mit den Normen $p^e n(B)$ bzw. $p^{e'} n(C)$, wobei e und e' möglichst kleine, nicht negative Exponenten sind, so daß es

maximale Gitter dieser Normen in $(Q_p^n)_0$ überhaupt geben kann. Ferner gilt der Satz ((1), Satz 9.4), daß sämtliche Vektoren z aus einem anisotropen Raum, für die $\frac{1}{2} z^2$ durch p^f teilbar ist, ein maximales Gitter der Norm p^f oder p^{f+1} bilden.

Daraus folgt, daß e und e' Null oder Eins sind.

Als Gitter aus N sind B und C isomorph, haben also dieselbe Norm: $p^r = p^s$. Ist $[x_1, \dots, x_u]$ die Basis von B_0 , so muß $t_1 = \dots = t_u = 0$ sein, da B_0 und C_0 nach obigem Satz maximale Gitter derselben Norm im gleichen anisotropen Raum, nach dem zweiten Satz also gleich sind. Aus $p^r = p^s$ folgt dann für die weiteren Basisvektoren $t_{u+2v-1} = -t_{u+2v}$.

Mit Hilfe dieser Basen konstruieren wir wieder ein Zwischengitter D' durch Angabe einer Basis:

$$D' = [x_1, \dots, x_u, px_{u+1}, p^{-1}x_{u+2}, \dots, px_{u+2v-1}, p^{-1}x_{u+2v}, \dots]$$

Es gelten dann die Abstandsbeziehungen $d(B, D') = 1$ und

$d(D', C) < d(B, C)$, aber D' liegt jetzt im allgemeinen nicht mehr in N . Dafür zeigt die spezielle Art der Basen von B und C , mit deren Hilfe D' konstruiert wurde, daß D' wenigstens dieselbe Norm und dieselbe reduzierte Determinante wie B und C hat. Dies wollen wir ausnützen. Wir bezeichnen daher die Menge aller Gitter aus M , die gleiche Norm und gleiche reduzierte Determinante wie die Gitter in N haben, mit $\bar{N}$ und nennen zwei Gitter aus $\bar{N}$ äquivalent, wenn es ein Element aus $O_n(Z_S, s)$ gibt, das sie ineinander überführt. Wir wollen zeigen, daß $\bar{N}$ in endlich viele Klassen äquivalenter Gitter zerfällt, von denen dann eine N ist. Dazu definieren wir für ein beliebiges Gitter X aus $\bar{N}$ wieder ein

Gitter $\bar{X}$ aus Q^n durch $\bar{X} = \bigcap_{q \neq p} (\bar{A}_q \cap Q^n) \cap X$; dabei ist $\bar{A}_q = \bar{A} \otimes_{\mathbb{Z}} \mathbb{Z}_q$. Da sich Norm und reduzierte Determinante eines Gitters aus Q^n multiplikativ aus denen der q -adischen Hüllen zusammensetzen, haben auch alle so gewonnenen Gitter $\bar{X}$ gleiche Norm und gleiche reduzierte Determinante. Von Gittern in Q^n mit dieser Eigenschaft ist aber bekannt, daß sie sich auf endlich viele Isomorphieklassen verteilen ((1), Satz 12.7); nach Definition gibt es zu zwei Elementen derselben Klasse ein Element aus $O_n(Q, s)$, das sie ineinander überführt. Für die Gitter $\bar{X}$ muß dieses Element dann sogar in $O_n(\mathbb{Z}_{\{p\}}, s)$, also erst recht in $O_n(\mathbb{Z}_S, s)$ liegen. Es bildet dann auch die p -adischen Hüllen $X = \bar{X} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ aufeinander ab und damit ist unsere Behauptung bewiesen.

Für die Äquivalenzklassen in $\bar{N}$ wählen wir nun ein vollständiges Vertretersystem V . Wegen der Endlichkeit von V existiert eine Konstante d , der Durchmesser von V , so daß zwei beliebige Gitter aus V höchstens den Abstand d haben. Dann läßt sich aber auch zu beliebig vorgegebenem Gitter X aus $\bar{N}$ und beliebig vorgegebener Äquivalenzklasse H ein Gitter Y aus H mit $d(X, Y) \leq d$ finden, wie man durch Anwendung eines Elementes aus $O_n(\mathbb{Z}_S, s)$ auf die zugehörigen Vertreter in V zeigt.

Jetzt sind wir in der Lage, die Bedingung 3a) für die Menge N nachzuweisen. Ist d der Durchmesser von V , so setzen wir $K = 2d + 1$. Wenden wir unser Konstruktionsverfahren von Zwischengittern $(d+1)$ -mal hintereinander an, so erhalten wir zu zwei beliebigen Gittern B und C aus N mit $d(B, C) > K$ ein Gitter D' aus $\bar{N}$ mit $d(B, D') \leq d+1$ und $d(D', C) \leq d(B, C) - (d+1)$.

Zu D'' existiert aber ein Gitter D aus N mit $d(D'', D) \leq d$ und somit ergibt sich für D :

$$d(B, D) \leq d(B, D'') + d(D'', D) \leq d + 1 + d = K$$

$$d(D, C) \leq d(D, D'') + d(D'', C) \leq d + d(B, C) - (d+1) < d(B, C).$$

Um die Bedingung 4a) erfüllen zu können, müssen wir eine größere Konstante K wählen, nämlich $K = 4d + 1$. Seien B, C, D drei Gitter aus N , deren gegenseitige Abstände größer als K sind. Ausgehend von B und C liefert die mehrfache Anwendung unseres Konstruktionsverfahrens ein Gitter E' aus $\bar{N}$ mit $d(B, E') \leq 2d + 1$ und $d(E', C) \leq d(B, C) - (2d+1)$, sowie $d(E', D) \leq \max \{d(B, D), d(C, D)\}$ und nochmals auf E' und D angewandt ein Gitter E'' aus $\bar{N}$ mit $d(E'', E') \leq d$ und $d(E'', D) \leq d(E', D) - d$. Zu E'' endlich gibt es ein Gitter E aus N mit $d(E'', E) \leq d$ und E hat alle verlangten Eigenschaften:

$$d(B, E) \leq d(B, E') + d(E', E'') + d(E'', E) \leq (2d+1) + d + d = K$$

$$d(E, C) \leq d(E, E'') + d(E'', E') + d(E', C) \leq d + d + d(B, C) - (2d+1) < d(B, C)$$

$$d(E, D) \leq d(E, E'') + d(E'', D) \leq d + d(E', D) - d \leq \max \{d(B, D), d(C, D)\}.$$

Es bleibt noch der Fall zu betrachten, daß das Gitter A nicht maximal ist. Wir können dann aber zu A ein maximales Gitter A' finden, das A umfaßt; sein Abstand von A möge H heißen. Die Menge N erhielten wir durch Anwendung der Gruppe $O_n(Z_S, s)$ auf A ; wenden wir dieselbe Gruppe auf A' an, so erhalten wir zu jedem Gitter B aus N ein maximales Gitter B' , das B umfaßt. Dabei ist für jedes B der Abstand $d(B, B')$ konstant gleich H . Da die ge-

gestrichenen Gitter den Bedingungen 3a) bzw. 4a) genügen, kann man leicht nachrechnen, daß sie auch von den ungestrichenen erfüllt werden, natürlich mit größeren Konstanten K. Wir wollen dies für Bedingung 3a) durchführen und zeigen, daß man mit der Konstanten $K' = 2H + (4H+1)K + 1$ auskommt. Seien B und C also zwei Gitter aus N, deren Abstand größer als K' ist. Dann existieren maximale Gitter B' und C' mit $d(B, B') = H$ und $d(C, C') = H$ und aus $d(B, C) > K'$ folgt auf Grund der Ungleichung $d(B', C') \geq d(B, C) - d(B, B') - d(C, C') = d(B, C) - 2H$, daß $d(B', C')$ größer als $(4H+1)K + 1$ ist, so daß man den ersten Teil von Bedingung 4a) wenigstens $(4H+1)$ -mal auf die gestrichenen Gitter anwenden kann. Die $(4H+1)$ -malige Anwendung (ausgehend von B' und C') liefert ein Gitter D' und das zugehörige Gitter D aus N mit $d(D, D') = H$. Für D folgt jetzt leicht:

$$\begin{aligned} d(B, D) &\leq d(B, B') + d(B', D') + d(D', D) \leq H + (4H+1)K + H < K' \\ d(C, D) &\leq d(C, C') + d(C', D') + d(D', D) \leq H + d(C', B') - (4H+1)H \\ &\leq 2H - (4H+1) + d(C, C') + d(C, B) + d(B, B') \\ &\leq d(C, B) + 2H + 2H - (4H+1) < d(C, B). \end{aligned}$$

Die Bedingungen 4a) weist man durch eine ähnliche Rechnung nach; dazu ist kein neuer Beweisgedanke nötig, deshalb sei nur vermerkt, daß man als Konstante $2H + K + 8HK + 4HK^2 + 1$ wählen kann(dabei ist K jetzt die Konstante aus 4a) für die gestrichenen Gitter).

Abschnitt III:

AUSDEHNUNG DER RESULTATE AUF EINIGE WEITERE GRUPPEN.

Die linearen und orthogonalen Einheitengruppen, die wir bisher betrachteten, waren typische Anwendungsbeispiele der Sätze 1 - 4. Wir können auf dieselbe Weise auch noch für einige andere Sorten von Einheitengruppen zeigen, daß sie durch endlich viele Elemente erzeugt und durch endlich viele Relationen zwischen ihren Erzeugenden definiert werden können; wir werden diese Aussagen im Folgenden kurz als Eigenschaft E und R bezeichnen. Die Beweise sind den im vorigen Abschnitt geführten so ähnlich, daß wir uns damit begnügen können, die notwendigen Änderungen anzugeben.

1. Lineare und orthogonale Einheitengruppen über einem algebraischen Zahlkörper. Für die allgemeine lineare Gruppe über einem Zahlkörper K hat P. Humbert (in (3), S. 305) die endliche Erzeugbarkeit der gewöhnlichen Einheitengruppe $GL_n(\mu)$ bewiesen, das ist die Gruppe aller n -reihigen Matrizen mit Elementen aus dem Ring μ der ganzen Zahlen von K , deren Determinante eine Einheit von K ist. Der Beweis ist wieder eine Anwendung von Satz 1. Hat K g_1 reelle und g_2 komplexe unendliche Primstellen, so benützt man als Raum T einen Produktraum von $g_1 + g_2$ Faktoren und zwar nimmt man g_1 -mal den Raum der positiv definiten reellen quadratischen Formen und g_2 -mal den Raum der positiv definiten Hermiteschen Formen als Faktor. Insbesondere sieht man, daß T konvex ist, es läßt sich also auch wieder Eigenschaft R beweisen.

Bezeichnen wir mit S jetzt eine endliche Menge von Primdivisoren von K , so bildet die Menge aller Elemente aus K , in deren Primdivisorzerlegung alle nicht in S gelegenen Primdivisoren mit nicht negativem Exponenten auftreten, einen Ring $\mathcal{O}_S$. Zu S können wir die verallgemeinerte Einheitengruppe $GL_n(\mathcal{O}_S)$ definieren als die Untergruppe von $GL_n(K)$, deren Matrixelemente aus $\mathcal{O}_S$ entnommen sind und deren Determinante eine relative Einheit bezüglich S ist.

Mit Hilfe der Sätze 3 und 4 kann man wieder zeigen, daß die Gruppen $GL_n(\mathcal{O}_S)$ die Eigenschaften E und R besitzen. Der Beweis verläuft nach demselben Schema wie im vorigen Abschnitt. Ist $K_{\mathfrak{f}}$ die perfekte Hülle von K bezüglich des Primdivisors $\mathfrak{f}$, so definiert man die Menge M jetzt durch Anwendung von $GL_n(\mathcal{O}_S)$ auf das Einheitsgitter in $K_{\mathfrak{f}}^n$ und führt eine Metrik ein durch: $d(B, C) = \min s$ mit $\mathfrak{f}^s B \subseteq C$ und $\mathfrak{f}^s C \subseteq B$. Bei der Konstruktion der Zwischengitter hat man anstelle der Primzahl p ein Primelement π aus $K_{\mathfrak{f}}$ zu nehmen. Die einzige zusätzliche Schwierigkeit rührt davon her, daß die Klassenzahl des Körpers K im allgemeinen nicht mehr gleich Eins ist. Als Folge davon brauchen die Zwischengitter D nicht mehr in M zu liegen, da die zugehörigen Gitter $\bar{D}$ in K^n im allgemeinen keine Basis mehr haben (vgl. Seite 25). Einen Ersatz liefert eine Konstruktion, die auf Steinitz zurückgeht (siehe (10a), S. 358-59 und auch (1), Satz 12.5): Zu einem vorgegebenem Gitter J in K^n gibt es $(n-1)$ linear unabhängige Vektoren $i_1, \dots, i_{n-1}$ aus J und einen von diesen unabhängigen Vektor i_n aus K^n , sowie ein Ideal $\mathfrak{m}$ aus K , so daß die

Menge der Vektoren x aus J identisch ist mit der Menge der Vektoren $x = \sum_{k=1}^n x_k i_k$, wobei $x_1, \dots, x_{n-1}$ ganz sind und x_n Vielfaches von m ist. Dabei ist die Idealklasse von m durch das Gitter festgelegt und zwei Gitter J und J' können genau dann durch ein Element aus $GL_n(K)$ ineinander übergeführt werden, wenn m und m' in derselben Idealklasse liegen. Da die Klassenzahl von K endlich ist, hat man dieselbe Situation wie in Abschnitt II.3 bei den orthogonalen Gruppen: die zunächst mit Hilfe von Basen konstruierten Zwischengitter liegen in einer Menge $\overline{M}$, die in endlich viele Klassen zerfällt, von denen eine M ist. Genau wie dort kann man dann den Beweis zu Ende führen.

Eine Übertragung des Humbertschen Resultates auf die spezielle lineare Gruppe scheint nicht bekannt zu sein.

Für die orthogonalen Gruppen $O_n(K, s)$ zu einer quadratischen Form s über dem Zahlkörper K hat Ramanathan die endliche Erzeugbarkeit der gewöhnlichen Einheitengruppen $O_n(\mu, s)$ bewiesen (in (8), S.241 und (9), S.6). Auch er wendet Satz 1 an. Als Raum T verwendet er eine Mannigfaltigkeit W in dem oben beschriebenen Produktraum von Humbert. Dabei ist W selbst direktes Produkt von Mannigfaltigkeiten W_i in den einzelnen Faktoren. Die W_i werden gegeben durch die Gleichungen $h s_i^{-1} h = s_i$ für die reellen bzw. $\bar{h} s_i^{-1} h = \bar{s}_i$ für die komplexen Primstellen; dabei bezeichnet s_i die i -te Konjugierte der quadratischen Form s . Auch W ist wieder konvex, so daß auch Eigenschaft R folgt.

Behauptung und Beweis für die verallgemeinerten Einheitengruppen

pen $O_n(\mathcal{O}_S, s)$ kann man wörtlich aus Abschnitt II.3 übernehmen, wenn man stets Primzahl durch Primdivisor bzw. Primelement ersetzt. Die dort benützten Sätze gelten nämlich ohnehin für beliebige Zahlkörper.

2. Unitäre und symplektische Einheitengruppen. Die unitären und symplektischen Gruppen werden bekanntlich wie die orthogonalen durch Matrizengleichungen definiert. Ist K ein Körper mit einem involutorischem Automorphismus J , so heißt eine Matrix h mit Elementen aus K Hermitesch bezüglich J , wenn sie die Gleichung $h^T = h^J$ erfüllt und die Lösungen x der Gleichung $x^T h x^J = h$ bilden die unitäre Gruppe bezüglich h . Die symplektische Gruppe wird für schiefsymmetrische Matrizen t durch die Gleichung $x^T t x = t$ definiert (wir betrachten hier nur gerade Dimensionen, da t sonst singulär ist).

Hier können wir unsere Sätze nicht für einen beliebigen algebraischen Zahlkörper aussprechen, da die endliche Erzeugbarkeit der gewöhnlichen Einheitengruppen bis jetzt anscheinend nur für Spezialfälle bewiesen wurde (es gibt allerdings eine sehr allgemeine Beweisskizze von Ramanathan in (10)).

Für die unitären Gruppen ist der Fall einer imaginär quadratischen Erweiterung K eines total reellen Zahlkörpers K' behandelt worden; als Automorphismus J hat man hier den Übergang zur konjugiert komplexen Zahl zu wählen. Ramanathan hat gezeigt, daß sich in diesem Fall der Beweis genauso wie für die orthogonalen Gruppen führen läßt ((8), S.241). Man benützt nämlich wieder die Produktmannigfaltigkeit W und zwar wird für

jede reelle Primstelle von K' durch die Gleichung $xh_1^{-1}x = h_1$ ($h_1 = i$ -te Konjugierte von h) ein Faktor definiert; die Elemente eines Faktors sind natürlich jetzt komplexe Matrizen. Aus der Konvexität von W folgt auch für die betrachteten unitären Einheitengruppen wieder Eigenschaft R.

In allen Fällen, in denen man für die gewöhnlichen unitären Einheitengruppen die Eigenschaften E und R nachweisen kann, gelingt es auch, sie für die verallgemeinerten zu beweisen. Um dies zu belegen, wollen wir kurz zeigen, daß auch hier wieder die Sätze 3 und 4 anwendbar sind, sobald man die Induktionsverankerung hat.

Bei der Definition der verallgemeinerten Einheitengruppen ist folgendes zu beachten: Ist K' der Fixkörper der Involution J , so bezeichnet S nunmehr eine endliche Menge von Primdivisoren von K' . K ist quadratische Erweiterung von K' . Die Primdivisoren von K' können bei dieser Erweiterung träge bleiben, sich verzweigen oder sich zerlegen: $\mathfrak{y} = \mathfrak{P}$, $\mathfrak{y} = \mathfrak{P}^2$, $\mathfrak{y} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$. Den letzten Fall haben wir im Folgenden immer gesondert zu betrachten. Wir haben zunächst anzugeben, in welchen Vektorräumen wir die Gitter wählen, die uns zur Definition der Räume M dienen. In den beiden ersten Fällen nehmen wir den Raum $K_{\mathfrak{P}}^n$, im letzten Fall den n -dimensionalen Vektorraum über der direkten Summe $K'_{\mathfrak{y}} \oplus K'_{\mathfrak{y}}$ (ihre Elemente bezeichnen wir mit (a, b)). Die beiden Summanden des Vektorraums müssen wir auseinander halten, d.h. wir setzen $(K'_{\mathfrak{y}} \oplus K'_{\mathfrak{y}})^n = R_1 \oplus R_2$, wobei R_1 und R_2 isomorph zu $K_{\mathfrak{y}}'^n$ sind. Ist $\Gamma_{\mathfrak{y}}$ der Ring der ganzen $\mathfrak{y}$ -adischen Elemente von $K'_{\mathfrak{y}}$, so bezeichnen wir $\Gamma_{\mathfrak{y}} = \Gamma_{\mathfrak{y}}' \oplus \Gamma_{\mathfrak{y}}'$ als den Ring der ganzen Elemente

von $K'_4 \oplus K'_j$, bezüglich dessen wir die Gitter definieren. Ist B ein Gitter, so bezeichnen wir die Teilgitter $B \cap R_1 = (1,0) \cdot B$ und $B \cap R_2 = (0,1) \cdot B$ mit B_1 bzw. B_2 ; dann ist $B = B_1 \oplus B_2$. B_1 und B_2 können wir als Γ'_4 -Moduln auffassen. Durch die vorgegebene Hermitesche Form h werden die genannten Vektorräume zu metrischen Räumen (im letzten Fall wird die Involution J zur Vertauschung der beiden Summanden). Die Räume M werden wieder als die Mengen von Gittern definiert, die durch Anwendung der jeweils gegebenen Einheitengruppe auf das Einheitsgitter entstehen. Die Metrik in M führen wir so ein: $d(B,C) = \min s$ mit $p^s B \subseteq C \subseteq p^{-s} B$ bzw. $d(B,C) = \min \max (s,t)$ mit $y^s B_1 \subseteq C_1 \subseteq y^{-s} B_1$ und $y^t B_2 \subseteq C_2 \subseteq y^{-t} B_2$ im 3. Fall. Der Beweis für die Anwendbarkeit der Sätze 3 und 4 kann nun völlig analog zu dem in Abschnitt II.3 durchgeführt werden (insbesondere werden die dortigen Begriffe übernommen). Man braucht also einmal Ersatz für die aus (1) entnommenen Sätze 9.4 und 9.5, zum anderen die Endlichkeit der Klassenzahl für Hermitesche Formen.

Für den Fall eines trägen oder verzweigten Primdivisors lassen sich die genannten Sätze vollständig übertragen:

- a) Sämtliche Vektoren x aus einem perfekten anisotropen Raum K^n , für welche $\frac{1}{2} h(x,x)$ durch y^f teilbar ist, bilden ein maximales Gitter der Norm y^f oder y^{f+1} .
- b) π sei ein Primelement von K_p . Zwei maximale Gitter B und C aus K_p^n besitzen Basen x_i und $y_i = \pi^{t_i} x_i$, deren Skalarproduktmatrizen direkte Summen von einer Matrix des jeweiligen anisotropen Kerns und zweireihigen Matrizen der Form $\begin{pmatrix} 0 & a \\ a^J & 0 \end{pmatrix}$ sind. Dabei ist $a = \pi^b$ für B bzw. $a = \pi^c$ für C und

$\frac{1}{2} (a + a^J)$ ist gleich der Norm des jeweiligen Gitters. Die anisotropen Kerne sind maximale Gitter kleinstmöglicher Norm in einem anisotropen Teilraum von K_F^n .

Bei a) genügt es zu beweisen, daß mit $\frac{1}{2} h(a,a)$ und $\frac{1}{2} h(b,b)$ auch $\frac{1}{2} h(a+b,a+b)$ ganz ist. Hierzu zeigt man genau wie in (1), daß aus der Annahme des Gegenteils folgt, daß die quadratische Form $[h(a,b) + h(a,b)^J]^{-1} h(xa+yb, xa+yb)$ mit x,y aus K_F' die Null darstellt.

Auch der Beweis von b) läßt sich genau wie der entsprechende in (1) führen. Man hat zusätzlich nur die folgende Behauptung zu beweisen: Ist x_1 ein isotroper Vektor aus B und liegt $\pi^{-1} x_1$ nicht in B, so gibt es einen Vektor y_1 aus B, so daß $h(x_1, y_1)$ alle Ausdrücke $h(x,y)$ mit x und y aus B teilt. Beim Beweis können wir annehmen, daß die Norm von B gleich $\mathfrak{f}^0 = (1)$ ist (sonst multipliziert man die Form h mit einem geeigneten Faktor). Bezeichnet $\mathfrak{f}$ die Differentiale von K_F/K_F' , so sind dann alle Ausdrücke $h(x,y)$ mit x,y aus B Vielfache des Divisors $\mathfrak{a} = (2) \mathfrak{f}^{-1}$ (denn bekanntlich kann man die Differentiale folgendermaßen definieren: Die Menge aller Elemente a aus K_F für die die Relativspur von K_F bzgl. K_F' von ag für beliebiges ganzes g aus K_F ganz ist, bildet die Menge der Vielfachen eines Divisors $\mathfrak{f}^{-1}$ mit ganzem $\mathfrak{f}$ und $\mathfrak{f}$ nennt man die Differentiale von K_F/K_F'). Der g.g.T. aller Ausdrücke $h(x_1, y)$ mit y aus B sei der Divisor $\mathfrak{L}$. Wäre $\mathfrak{a}$ echter Teiler von $\mathfrak{L}$, dann könnte man das Gitter B durch Hinzunahme von $\pi^{-1} x_1$ erweitern, ohne - nach Definition der Differentiale - die Norm zu verkleinern. Das widerspricht aber der vorausgesetzten Maximalität

von B und somit ergibt sich die Behauptung.

Im Fall eines zerlegten Primdivisors $\mathfrak{p}$ kommen wir mit einem etwas einfacheren Satz aus:

B und C seien zwei maximale Gitter in $R_1 \oplus R_2$, $B = B_1 \oplus B_2$ und $C = C_1 \oplus C_2$; ihre Normen seien (π^b) bzw. (π^c) , π bezeichne ein Primelement von K_2' . Dann gilt:

Es gibt Vektoren x_i aus B_1 und y_i aus B_2 sowie ganze Zahlen s_i und t_i ($i=1, \dots, n$), so daß die Vektoren $x_i + y_i$ eine Basis von B und die Vektoren $\pi^{s_i} x_i + \pi^{t_i} y_i$ eine Basis von C bilden. Dabei ist $\frac{1}{2} h(x_i + y_i, x_k + y_k) = \delta_{ik} \cdot \pi^b$ und $\frac{1}{2} h(\pi^{s_i} x_i + \pi^{t_i} y_i, \pi^{s_k} x_k + \pi^{t_k} y_k) = \delta_{ik} \pi^c$ (δ_{ik} bezeichnet das Kroneckersymbol). Die Zahlen s_i und t_i genügen den Gleichungen $s_i + t_i = c - b$ für alle i.

Beim Beweis wollen wir wieder voraussetzen, daß die Norm von B gleich (1) ist (d.h. $b = 0$). Wegen der Maximalität von B folgt dann, daß B_2 identisch ist mit dem bezüglich h dualen Gitter zu B_1 in R_2 , d.h. mit der Menge aller Vektoren y aus R_2 , für die $\frac{1}{2} [h(x, y) + h(x, y)^J]$ ganz ist für alle x aus B_1 (das duale Gitter existiert, weil wir nur nicht ausgeartete Formen h betrachten). Entsprechend ist C_2 das π^c -fache des dualen Gitters von C_1 , wenn (π^c) die Norm von C ist. Nach dem Elementarteilersatz gibt es nun Vektoren x_i aus B_1 und ganze Zahlen s_i , so daß die Vektoren x_i bzw. $\pi^{s_i} x_i$ Basen von B_1 bzw. C_1 bilden. Zu den x_i läßt sich ferner eine duale Basis finden, d.h. es gibt Vektoren y_i aus B_2 mit $\frac{1}{2} [h(x_i, y_k) + h(x_i, y_k)^J] = \delta_{ik}$. Die Vektoren $\pi^{t_i} y_i$ mit $t_i = c - s_i$ bilden dann eine Basis von C_2 . Damit ist alles gezeigt.

Mit diesen Sätzen hat man nun wieder die Möglichkeit Zwischengitter zu konstruieren. Schließlich braucht man noch die Endlichkeit der Klassenzahl für Hermitesche Formen. Diese ergibt sich durch Übertragung des Beweises von Satz 12.7 in (1) (man vgl. auch (4), S.62). Damit sind alle gegenüber Abschnitt II.3 nötigen Änderungen angegeben.

Zuletzt wollen wir noch die symplektische Gruppe betrachten. Hier folgt für den Fall des rationalen Zahlkörpers die endliche Erzeugbarkeit der gewöhnlichen symplektischen Einheitengruppe aus der Arbeit (13) von Siegel, wenn man in der dortigen Bezeichnungsweise (siehe (13), p.5) für die Gruppe $\Delta(\eta, h)$ den Fall $\eta = t$, $h = it$, $h = 1$, $r = 1$ wählt (t ist die vorgegebene schiefsymmetrische Matrix). Die für die Eigenschaft R benötigte Konvexität des Raums T , auf dem die Einheitengruppe operiert, folgt aus den Formeln auf Seite 46 und 47 sowie Lemma 6 in (13).

Betrachtet man die verallgemeinerten Einheitengruppen, so lassen sich die Sätze 3 und 4 wieder stets dann anwenden, wenn man die Induktionsverankerung durch die gewöhnliche Einheitengruppe hat. Die nötigen Hilfssätze ergeben sich hier leichter, da der ~~anisotrope~~ Anteil wegfällt.

Die Endlichkeit der Klassenzahl erhält man aus der in Satz 12.6 in (1) angegebenen Normalform für maximale Gitter über einem algebraischen Zahlkörper K : Ein maximales Gitter A ist direkte Summe von Gittern $A_i = [\nu_i, \delta_j]$, dabei sind i und j Vektoren aus K^n mit $t(i, j) = -t(j, i) = 1$ und die Vektoren aus A_i haben

die Gestalt $x_i + y_j$ mit x aus $\mathfrak{r}$ und y aus $\mathfrak{s}$ für Ideale $\mathfrak{r}$ und $\mathfrak{s}$ aus K . Wählt man diese Ideale noch aus einem festen Vertretersystem von Idealklassen, so folgt die Behauptung für maximale Gitter und andere kamen in unseren Beweisen auch nicht vor. Satz 9.4 aus (1) wird hier überflüssig, weil keine anisotropen Vektoren auftreten. Die Norm eines Gitters A definiert man nun als g.g.T. aller Ausdrücke $t(x,y)$ mit x und y aus A . Dann überträgt sich Satz 9.5 aus (1) beinahe wörtlich; in den Skalarproduktmatrizen treten natürlich jetzt Vorzeichen auf, die zweireihigen direkten Summanden haben die Gestalt $\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$ mit $a = n(A)$.

LITERATURVERZEICHNIS.

- (1) M.Eichler: Quadratische Formen und orthogonale Gruppen,
Springer Verlag 1952
- (2) M.Gerstenhaber: On the algebraic structure of discontinuous
groups, Proc. of the Am.Math.Soc.4, p.745-
750 (1953)
- (3) P.Humbert: Théorie de la réduction des formes quadra-
tiques définies positives dans un corps algé-
brique K fini, Comm.Math.Helv.12, p.263-306 (1940)
- (4) P.Humbert: Réduction des formes quadratiques dans un
corps algébrique fini, Comm.Math.Helv.23,
p.50-63 (1949)
- (5) A.G.Kurosch: Gruppentheorie, Berlin 1953.
- (6) H.Minkowski: Diskontinuitätsbereich für arithmetische
Äquivalenz, Crelle-Journal 129, S.220
- (7) H.Minkowski: Gesammelte Abhandlungen, Band 2, S.53-100.
- (8) K.G.Ramanathan: The theory of units of quadratic and
Hermitian forms, Am.Journal of Math.73,
p.233-255 (1951)
- (9) K.G.Ramanathan: Units of quadratic forms, Ann. of Math.56,
p.1-10 (1952)
- (10) K.G.Ramanathan: Units of Fixed Points in Involutorial
Algebras, Proc. of the International Sympo-
sium on Algebraic Number Theory, p.103-106
Tokyo 1955.

- (10a) I.Schur: Über Gruppen linearer Substitutionen mit
Koeffizienten aus einem algebraischen Zahl-
körper, Math. Annalen 71, S.355-367 (1912)
- (11) C.L.Siegel: Einheiten quadratischer Formen, Abh.Math.
Sem.Univ,Hamburg 13, S.209-239 (1940)
- (12) C.L.Siegel: Discontinuous groups, Annals of Math. 44,
p.674-689 (1943)
- (13) C.L.Siegel: Symplectic Geometry, Am.Journal of Math.65,
p.1-86 (1943)
- (14) H.Weyl: Algebraic Theory of Numbers, Princeton 1940

Lebenslauf.

Am 31. Januar 1935 wurde ich in München-Großhadern als einziges Kind des Werkmeisters Martin Behr und seiner Ehefrau Wilhelmine, geb. Bogner geboren. Ich gehöre der evangelisch-lutherischen Kirche an.

Von 1941 bis 1945 besuchte ich die Volksschule in München-Großhadern und in Ebenhausen bei Ingolstadt. Gegen Ende des Jahres 1945 trat ich in die Oberrealschule Ingolstadt ein, die ich 8 Jahre besuchte. Dort legte ich auch im Juli 1953 die Reifeprüfung ab.

Seit November 1953 studiere ich an der Universität München Mathematik und Physik. Ich hörte Vorlesungen bei den Professoren G. Aumann, F. Bopp, W. Britzelmayer, W. Gerlach, W. Heisenberg, M. Kneser, W. Maak, O. Perron, H. Richter, W. Rollwagen, R. Schmidt und K. Stein und bei den Dozenten D. Bierlein, H. Röhrle und E. Thoma.

Im Herbst 1958 habe ich das Staatsexamen in Mathematik und Physik für das Lehramt an Höheren Schulen in Bayern abgelegt. Vom pädagogischen Seminar ließ ich mich jedoch beurlauben, um Zeit für wissenschaftliches Arbeiten zu haben.

Vom Wintersemester 1957/58 bis zum Sommersemester 1960 war ich am Mathematischen Institut der Universität München als Hilfsassistent beschäftigt, seit 16.9.1960 bin ich dort als Verwalter einer wissenschaftlichen Assistentenstelle tätig.

Ingolstadt, den 3.1.1961

Helmut Behr

